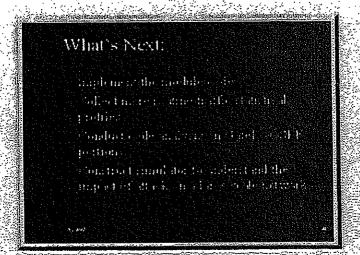
Case 1:04-cv-01199-SLR Document 509-10 Filed 05/20/2008 Page 1 of 20

PP Presentation









http://web.archive.org/web/1997/1077113049/www.mcnc.org/HTML/ITD/ANR/sn/sld030/htm

Scalable Intrusion Detection for the Emerging Network Infrastructure

1 of 1

Scalable Intrusion Detection for the Emerging Network Infrastructure

Scalable Intrusion Detection for the Emerging Network
Infrastructure

Y. Frank Jou S. Felix Wu

MENONESU

IDS Program Review

Next slide Back to the first slide. View Graphic Version

http://web.archive.org/web/19971017122825/www.mcnc.org/ATML/LTD/ANH/sri/tsid001.htm

Project Update:

Project Update

Project Update

- Overview
- System Architecture Design
- Routing Testbed Configuration
- Routing Traffic Statistical Profiles
- · Routing Attacks
- What's next ...

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/19971017123005/www.anchc.org/HTMI/ITD/ANR/srl/tsld002.htm

PP Presentation

PP Presentation

Overview: Target Environment

Previous slide Next slide Back to the first slide View Graphic Version

http://web-archive.org/web/19971017123106/www.inchc.org/HTML/ITD/ANR/spi/tsldi003.htm.

PP Presentation

PP Presentation

Overview: JiNao Architecture

- Integration of attack prevention (configurable firewall) and intrusion detection.
- Detect your neighbors.
- A RSMM (Remote Security Management Module) can coordinate a set of JiNao's to detect orchestrated attacks and isolate bad routers.

25 No. 1 (1)			The same of the sa
Previous slide	Novice de la constante de la c	- Reports the tire chile.	View Graphic Version
THE VEGULA DIRECT		Duote to morning	The state of the s
The state of the s	THE PARTY OF THE P	A self of the restriction of the strength of the contraction of the co	The same of the control of the contr

http://web.archive.org/web/19971017123206/www.menc.org/HTML/ITD/ANR/sci/Isld004.htm

Case 1:04-cv-01199-SLR Document 509-10 Filed 05/20/2008 Page 6 of 20

System Design:

System Design: & Block Diagram

System Design: of Block Diagram

Prevention Module

Detection Module

Decision Module

RSMM

SNMPv3 Eng.

Security

Officer

Previous slide Next slide

Back to the first slide View Graphic Version

http://web.archive.org/web/19971017.1233.06/www.mcnc.org/HTML/TTD/ANR/sri/isid005.htm

System Design; Intercept. Mod.

System Design: Intercept. Mod.

System Design: Intercept. Mod.

- May be placed in multiple protocol layers
 - Device driver
 - IP/IPSEC
 - o Higher-layer protocols
- May facilitate active intrusion detection.
 - o Catch-and-Trap (through RSMM)
- May timestamp the packet

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/19971017123404/www.mcnc.org/HFML/ITD/ANR/sni/tsld006.htm

PP Presentation

PP Presentation

System Design: Prevention Mod.

- Prevention Layer, Go or No-Go
 - Quick response
- Extraction Layer
 - o PDU format conversion
 - Multiple interception points correlation.
 - e.g. This SNMPng/v3 PDU as from /dev/eth1 and /dev/tunnel

Previous slide Next slide Back to the first slide View Graphic Version

PP Presentation

PP Presentation

System Design: Protocol Analysis

- Maintain a set of Finite-State Machines
 - o One FSM for each identified intrusion
- Provide extensibility
 - Reconfigurable at Run-Time
 - Table-driven implementation of FSMs
 - With a generic driver routine.
 - Use Concurrency Workbench (CWB) to produce the FSMs.

Previous slide Next slide ... Back to the first slide View Graphic Version

http://web.archive.org/web/19971017123601/www.mcnc.org/HTML/ITD/ANR/sri/tsld008.htm

Case 1:04-cv-01199-SLR Document 509-10 Filed 05/20/2008 Page 10 of 20

DP Presentation

PP Presentation

System Design: Statistical Analysis

- Unknown vulnerability detection
 - o Complementary to rule-based and protocol-based analysis
- Profile training
 - Comparing short-term vs. long-term behaviors
 - Weighted aging: Favor more recent observation.
 - o Experimenting with NIDES statistical algorithm

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/19971017123658/www.mcne.org/HTML/ITD/ANR/sri/Istd009-htm

PP Presentation

PP Presentation

System Design: Decision Mod.

- Make decisions on intrusion based on input from Prev/Detec Modules and RSMM
- Provide information for the LAM (RSMM)
- Propagate global information to the Prev/Detec Modules
 Notify security officer of faults/intrusion

۲.	Previous slide Next s	America - Commencer in the		The state of the s
٠,	Previous slide Next S	nde Baciete	Hine-Hiseshoe	A ICAN CITADETIC A CESTOR
٠.				Land to the control of the second the second to the second

PP Presentation

PP Presentation

Router A

Router B

Correlate Input to make informed decision

Previous slide Next slide Back to the first slide View Graphic Version

http://web;archive.org/web/19971017123855/www.monc.org/HTML/ITD/ANR/sti/isld011.htm

PP Presentation.

PP Presentation

System Design: Info. Abst. Mod.

- Detection Info. aggregation/MIB-fication
- o Run-length coding for data reduction for repeated normal report or persistent fault
- · Periodic checking and propagation of global information
- Scope of Impact representation
 - Topological info. on all the affected routers through graph representation (GrIDS?)

Previous slide Next slide Back to the first slide View Graphic Version

http://webjarchive.org/web/19971017123954/www.mcnc.org/HTML/1TD/ANR/sti/tsid012.htm

PP Presentation

PP Presentation

System Design: MIB

- Rule/FSM configuration and statistical parameter specification
- Local detection results
- Detection notifications
- Security control
- Log access

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/19971017124055/www.mcnc.org/HTML/ITD/ANR/sri/tsld013:htm:

PP Presentation

PP Presentation

System Design: RSMM

- SNMPv3 based management applications
- Access JiNao MIBs and correlate detection results
- Example: active intrusion detection (Catch and Trap)

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/1997101.7124153/www.mcnc.org/HTML/ITD/ANR/sti/isld014.htm

PP-Presentation

PP Presentation

Alice

Bob

Chris

RSMM

Active Intrusion Detection: Catch &

Trap

- **(1)**
- **(2)**
- (3)
- **(4)**
- (5)
- **(6)**

trap

- **(7)**
- (0)

suspend

http://web.archive.org/web/19971017124252/www.mcnc.org/HTML/ITD/ANR/sri/tsld015.htm

PP Presentation 2 of 2

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/1997-1017124252/www.menc.org/HEML/ITD/ANR/sh/4sld015.htm

Case 1:04-cv-01199-SLR Document 509-10 Filed 05/20/2008 Page 18 of 20

PP Presentation

PP Presentation

System Design: Interfaces

- Information exchange is done via message passing
 Authentication is provided if necessary
- Separate input queue for facilitating priority mechanisms

Previous slide Next slide	Back to the first slide View Graphic Versi	on.
STANDARD CONTRACTOR OF THE PARTY OF		

http://web.archive.org/web/19971017124351/www.mcnc.org/ATML/TTD/ANR/sti/isld016/htm

PP Presentation

PP Presentation

Testbed Configuration

- Two routing testbeds (autonomous systems, AS): MCNC & NCSU
- Each has three to four areas
- Allow independent code development
- Will be linked together to experiment ASBR attacks (only AS-external-LSAs are flooded throughout the entire AS)
- (Ref: configuration in file "testbed ps")

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/19971017124449/www.mcnc.org/HTML/ITD/ANR/sri/tsld017.htm

PP Presentation l of I

PP Presentation

Routing Statistical Profiles

- Hello packets: stable (like step-function)
 Database Description and LS Request packets: rare events (only for forming adjacencies)
- LS Update and LS Ack: periodic in about every 30 min (LSRefreshTime: 30 min; MinLSInterval.
- (Look for four other postscript files, two were normal, two were under attack)

Previous slide Next slide Back to the first slide View Graphic Version

http://web.archive.org/web/19971017124546/www.mene.org/ATML/1TD/ANR/stil/isld018.htm